

| |
|---|
| LODGED CLERK, U.S. DISTRICT COURT |
| 11/03/2023 |
| CENTRAL DISTRICT OF CALIFORNIA BY: AP DEPUTY |

UNITED STATES DISTRICT COURT

for the
Central District of California

| |
|---|
| FILED CLERK, U.S. DISTRICT COURT |
| 11/03/23 |
| CENTRAL DISTRICT OF CALIFORNIA BY: KC DEPUTY |

In the Matter of the Search of)
The person of REYES LEON MEZA, as)
described more fully in Attachment A-3.)
 Case No. 5:23-mj-00519

APPLICATION FOR A WARRANT BY TELEPHONE OR OTHER RELIABLE ELECTRONIC MEANS

I, a federal law enforcement officer or an attorney for the government, request a search warrant and state under penalty of perjury that I have reason to believe that on the following person or property (*identify the person or describe the property to be searched and give its location*):

See Attachment A-3

located in the Central District of California, there is now concealed (*identify the person or describe the property to be seized*):

See Attachment B

The basis for the search under Fed. R. Crim. P. 41(c) is (*check one or more*):

- evidence of a crime;
- contraband, fruits of crime, or other items illegally possessed;
- property designed for use, intended for use, or used in committing a crime;
- a person to be arrested or a person who is unlawfully restrained.

The search is related to a violation of:

| <i>Code Section</i> | <i>Offense Description</i> |
|-----------------------|---|
| 21 U.S.C. § 841(a)(1) | Possession with Intent to Distribute Controlled Substances and Distribution of Controlled Substances |
| 21 U.S.C. § 846 | Conspiracy and Attempt to Distribute Controlled Substances |

The application is based on these facts:

See attached Affidavit

- Continued on the attached sheet.

Delayed notice of _____ days (*give exact ending date if more than 30 days: _____*) is requested under 18 U.S.C. § 3103a, the basis of which is set forth on the attached sheet.

/s/ David J. Thompson

Applicant's signature

David J. Thompson, USPIS TFO

Printed name and title

Attested to by the applicant in accordance with the requirements of Fed. R. Crim. P. 4.1 by telephone.

Date: November 3, 2023

[Signature]

Judge's signature

Hon. Sheri Pym, U.S. Magistrate Judge

Printed name and title

City and state: Riverside, CA

AUSA: K. Afia Bondero (x2435)

ATTACHMENT A-3

PERSON TO BE SEARCHED

The person of REYES LEON MEZA ("MEZA"), date of birth January 6, 1980, with California Driver's License Number B8838054. MEZA's California Department of Motor Vehicle records list him as standing 5'10" tall with black hair and brown eyes.

The search of MEZA shall include any and all clothing and personal belongings, digital devices, backpacks, wallets, briefcases, purses, and bags that are within MEZA's immediate vicinity and control at the location where the search warrant is executed.

ATTACHMENT B

I. ITEMS TO BE SEIZED

1. The items to be seized are evidence, contraband, fruits, or instrumentalities of violations of 21 U.S.C. § 841(a)(1) (possession with intent to distribute controlled substances and distribution of controlled substances) and 21 U.S.C. § 846 (conspiracy and attempt to distribute controlled substances) (the "Subject Offenses"), namely:

- a. Any controlled substance, controlled substance analogue, or listed chemical;
- b. Items and paraphernalia for the manufacturing, distributing, packaging, sale, or weighing of controlled substances, including scales and other weighing devices, plastic baggies, food saver sealing devices, heat sealing devices, balloons, packaging materials, containers, and money counters;
- c. Items used in the packaging of currency for consolidation and transportation, such as money-counting machines, money wrappers, carbon paper, rubber bands, duct tape or wrapping tape, plastic wrap or shrink wrap, and plastic sealing machines;
- d. United States currency over \$1,000 or bearer instruments worth over \$1,000 (including cashier's checks, traveler's checks, certificates of deposit, stock certificates, and bonds) (including the first \$1,000), and data, records, documents, or information (including electronic mail, messages over applications and social media, and photographs) pertaining to, obtaining, possessing, using, applications for, or

transferring money over \$1,000, such as bank account records, cryptocurrency records and accounts;

e. Documents and records reflecting the identity of, contact information for, communications with, or times, dates or locations of meetings with co-conspirators, sources of supply of controlled substances, or drug customers, including calendars, address books, telephone or other contact lists, pay/owe records, distribution or customer lists, correspondence, receipts, records, and documents noting price, quantities, and/or times when drugs were bought, sold, or otherwise distributed, whether contained in hard copy correspondence, notes, emails, text messages, photographs, videos (including items stored on digital devices), or otherwise;

f. Records, documents, programs, applications and materials, or evidence of the absence of same, sufficient to show call log information, including all telephone numbers dialed from any of the digital devices and all telephone numbers accessed through any push-to-talk functions, as well as all received or missed incoming calls;

g. Records, documents, programs, applications or materials, or evidence of the absence of same, sufficient to show SMS text, email communications or other text or written communications sent to or received from any of the digital devices and which relate to the above-named violations;

h. Records, documents, programs, applications or materials, or evidence of the absence of same, sufficient to show instant and social media messages (such as Facebook,

Facebook Messenger, Snapchat, FaceTime, Skype, and WhatsApp),
SMS text, email communications, or other text or written
communications sent to or received from any digital device and
which relate to the above-named violations;

i. Audio recordings, pictures, video recordings, or
still captured images related to the purchase, sale,
transportation, or distribution of drugs;

j. Contents of any calendar or date book;

k. Global Positioning System ("GPS") coordinates and
other information or records identifying travel routes,
destinations, origination points, and other locations; and

l. Any digital device which is itself or which
contains evidence, contraband, fruits, or instrumentalities of
the Subject Offenses, and forensic copies thereof.

m. With respect to any digital device containing
evidence falling within the scope of the foregoing categories of
items to be seized:

i. evidence of who used, owned, or controlled
the device at the time the things described in this warrant were
created, edited, or deleted, such as logs, registry entries,
configuration files, saved usernames and passwords, documents,
browsing history, user profiles, e-mail, e-mail contacts, chat
and instant messaging logs, photographs, and correspondence;

ii. evidence of the presence or absence of
software that would allow others to control the device, such as
viruses, Trojan horses, and other forms of malicious software,

as well as evidence of the presence or absence of security software designed to detect malicious software;

iii. evidence of the attachment of other devices;

iv. evidence of counter-forensic programs (and associated data) that are designed to eliminate data from the device;

v. evidence of the times the device was used;

vi. passwords, encryption keys, biometric keys, and other access devices that may be necessary to access the device;

vii. applications, utility programs, compilers, interpreters, or other software, as well as documentation and manuals, that may be necessary to access the device or to conduct a forensic examination of it;

viii. records of or information about Internet Protocol addresses used by the device;

ix. records of or information about the device's Internet activity, including firewall logs, caches, browser history and cookies, "bookmarked" or "favorite" web pages, search terms that the user entered into any Internet search engine, and records of user-typed web addresses.

2. As used herein, the terms "records," "documents," "programs," "applications," and "materials" include records, documents, programs, applications, and materials created, modified, or stored in any form, including in digital form on any digital device and any forensic copies thereof.

3. As used herein, the term "digital device" includes any electronic system or device capable of storing or processing data in digital form, including central processing units; desktop, laptop, notebook, and tablet computers; personal digital assistants; wireless communication devices, such as telephone paging devices, beepers, mobile telephones, and smart phones; digital cameras; gaming consoles (including Sony PlayStations and Microsoft Xboxes); peripheral input/output devices, such as keyboards, printers, scanners, plotters, monitors, and drives intended for removable media; related communications devices, such as modems, routers, cables, and connections; storage media, such as hard disk drives, floppy disks, memory cards, optical disks, and magnetic tapes used to store digital data (excluding analog tapes such as VHS); and security devices.

II. SEARCH PROCEDURE FOR DIGITAL DEVICE(S)

4. In searching digital devices (or forensic copies thereof), law enforcement personnel executing this search warrant will employ the following procedure:

a. Law enforcement personnel or other individuals assisting law enforcement personnel (the "search team") will, in their discretion, either search the digital device(s) on-site or seize and transport the device(s) and/or forensic image(s) thereof to an appropriate law enforcement laboratory or similar facility to be searched at that location. The search team shall complete the search as soon as is practicable but not to exceed 120 days from the date of execution of the warrant. The

government will not search the digital device(s) and/or forensic image(s) thereof beyond this 120-day period without obtaining an extension of time order from the Court.

b. The search team will conduct the search only by using search protocols specifically chosen to identify only the specific items to be seized under this warrant.

i. The search team may subject all of the data contained in each digital device capable of containing any of the items to be seized to the search protocols to determine whether the device and any data thereon falls within the list of items to be seized. The search team may also search for and attempt to recover deleted, "hidden," or encrypted data to determine, pursuant to the search protocols, whether the data falls within the list of items to be seized.

ii. The search team may use tools to exclude normal operating system files and standard third-party software that do not need to be searched.

iii. The search team may use forensic examination and searching tools, such as "EnCase" and "FTK" (Forensic Tool Kit), which tools may use hashing and other sophisticated techniques.

c. The search team will not seize contraband or evidence relating to other crimes outside the scope of the items to be seized without first obtaining a further warrant to search for and seize such contraband or evidence.

d. If the search determines that a digital device does not contain any data falling within the list of items to be

seized, the government will, as soon as is practicable, return the device and delete or destroy all forensic copies thereof.

e. If the search determines that a digital device does contain data falling within the list of items to be seized, the government may make and retain copies of such data, and may access such data at any time.

f. If the search determines that a digital device is (1) itself an item to be seized and/or (2) contains data falling within the list of other items to be seized, the government may retain the digital device and any forensic copies of the digital device, but may not access data falling outside the scope of the other items to be seized (after the time for searching the device has expired) absent further court order.

g. The government may also retain a digital device if the government, prior to the end of the search period, obtains an order from the Court authorizing retention of the device (or while an application for such an order is pending), including in circumstances where the government has not been able to fully search a device because the device or files contained therein is/are encrypted.

h. After the completion of the search of the digital devices, the government shall not access digital data falling outside the scope of the items to be seized absent further order of the Court.

5. In order to search for data capable of being read or interpreted by a digital device, law enforcement personnel are authorized to seize the following items:

- a. Any digital device capable of being used to commit, further, or store evidence of the offense(s) listed above;
- b. Any equipment used to facilitate the transmission, creation, display, encoding, or storage of digital data;
- c. Any magnetic, electronic, or optical storage device capable of storing digital data;
- d. Any documentation, operating logs, or reference manuals regarding the operation of the digital device or software used in the digital device;
- e. Any applications, utility programs, compilers, interpreters, or other software used to facilitate direct or indirect communication with the digital device;
- f. Any physical keys, encryption devices, dongles, or similar physical items that are necessary to gain access to the digital device or data stored on the digital device; and
- g. Any passwords, password files, biometric keys, test keys, encryption codes, or other information necessary to access the digital device or data stored on the digital device.

6. The review of the electronic data obtained pursuant to this warrant may be conducted by any government personnel assisting in the investigation, who may include, in addition to law enforcement officers and agents, attorneys for the government, attorney support staff, and technical experts. Pursuant to this warrant, the investigating agency may deliver a complete copy of the seized or copied electronic data to the

custody and control of attorneys for the government and their support staff for their independent review.

1. During the execution of this search warrant, law enforcement is permitted to: (1) depress MEZA's thumb and/or fingers onto the fingerprint sensor of the device (only when the device has such a sensor), and direct which specific finger(s) and/or thumb(s) shall be depressed; and (2) hold the device in front of MEZA's face with his or her eyes open to activate the facial-, iris-, or retina-recognition feature, in order to gain access to the contents of any such device. In depressing a person's thumb or finger onto a device and in holding a device in front of a person's face, law enforcement may not use excessive force, as defined in Graham v. Connor, 490 U.S. 386 (1989); specifically, law enforcement may use no more than objectively reasonable force in light of the facts and circumstances confronting them.

7. The special procedures relating to digital devices found in this warrant govern only the search of digital devices pursuant to the authority conferred by this warrant and do not apply to any search of digital devices pursuant to any other court order.

AFFIDAVIT

I, David J. Thompson, being duly sworn, declare and state as follows:

I. PURPOSE OF AFFIDAVIT

1. This affidavit is made in support of a criminal complaint and arrest warrant against REYES LEON MEZA ("MEZA") for a violation of 21 U.S.C. § 841(a)(1), (b) (1) (C): Distribution of Fentanyl Resulting in Death.

2. This affidavit is also made in support of applications for warrants to search the following:

a. 12701 Lateen Dr., Moreno Valley, CA 92553 (the "SUBJECT PREMISES") as described more fully in Attachment A-1;

b. a red Mercedes Benz with California license plate 8VJF230 (the "SUBJECT VEHICLE"), as described more fully in Attachment A-2; and

c. the person of MEZA as described more fully in Attachment A-3.

3. The requested search warrants seek authorization to seize evidence, fruits, or instrumentalities of violations of 21 U.S.C. § 841(a)(1) (possession with intent to distribute controlled substances and distribution of controlled substances) and 21 U.S.C. § 846 (conspiracy and attempt to distribute controlled substances) (the "Subject Offenses"), as described more fully in Attachment B. Attachments A-1, A-2, A-3, and B are incorporated herein by reference.

4. The facts set forth in this affidavit are based upon my personal observations, my training and experience, and

information obtained from various law enforcement personnel and witnesses. This affidavit is intended to show merely that there is sufficient probable cause for the requested complaint, arrest warrant, and search warrants, and does not purport to set forth all of my knowledge of or investigation into this matter. Unless specifically indicated otherwise, all conversations and statements described in this affidavit are related in substance and in part only.

II. BACKGROUND OF AFFIANT

5. I am a Task Force Officer ("TFO") with the United States Postal Inspection Service ("USPIS") and have been so employed since December of 2021. I am currently assigned to the Contraband Interdiction and Investigations South Team of the Los Angeles Division, which is responsible for investigating drug trafficking violations involving the United States Mail and United States Postal Service employees. As such, I am an "investigative or law enforcement officer" of the United States within the meaning of Title 18, United States Code, Section 2510(7); that is, an officer of the United States empowered by law to conduct investigations of, and to make arrests for, offenses enumerated in Title 18, United States Code, Section 2516. Prior to being assigned as a TFO with the USPIS, I worked patrol and investigations as a full-time sworn law enforcement officer with the Chino Police Department ("CPD"). I have been a sworn law enforcement officer since October 2013. I am a Police Officer within the meaning of Section 830.1 of the California Penal Code.

6. I have received training and have experience investigating violations of state and federal narcotics and money laundering laws, including, but not limited to Title 21, United States Code, Sections 841, 846, 952, 959 and 963 and Title 18, United States Code, Section 1956(a). I have been involved in various electronic surveillance methods including state and federal wiretap investigations, the debriefing of informants and witnesses, as well as others who have knowledge of the manufacturing, distribution, transportation, storage, and importation of controlled substances and the laundering of drug proceeds.

7. I have participated in many aspects of drug investigations, including investigations into the smuggling of illegal drugs, money laundering, and extortion related to drug trafficking. I am familiar with narcotics traffickers' methods of operation, including the manufacturing, storage, transportation, and distribution of narcotics, the collection of money that represents the proceeds of narcotics trafficking, and money laundering. I am also familiar with the manner in which narcotics traffickers transport and distribute narcotics in areas they control. I am familiar with how drug traffickers utilize counter-surveillance techniques to avoid detection by law enforcement. I also know that drug traffickers often communicate with their drug-trafficking associates through the use of cellular telephones. I have become aware that more sophisticated drug trafficking networks now utilize the dark web, e-mail, Voice over Internet Protocol, video chat, internet

messaging services, and social networking sites to communicate with one another. During drug-related communications, traffickers often use coded or cryptic language to disguise the drug-related nature of their conversations.

III. SUMMARY OF PROBABLE CAUSE

8. On August 16, 2023, Chino Police Department ("CPD") officers investigated the death of an on-duty United States Postal Service ("USPS") mail carrier, J.Z. Inside J.Z.'s vehicle, law enforcement found white narcotics residue that later tested positive for fentanyl and cocaine, and J.Z.'s phone. J.Z.'s phone contained text messages arranging a drug deal that occurred about three hours prior to his time of death, and video footage from security cameras at the location of the drug deal showed J.Z. meeting an individual in a red Mercedes Benz sedan, later determined to be the SUBJECT VEHICLE. J.Z.'s death was determined to be from fentanyl toxicity.

9. As discussed below, significant evidence links MEZA to the distribution of the narcotics that J.Z. took, resulting in his death. Previously, in July 2019, MEZA was arrested for possession/transportation of drugs for sale after being found in possession of about 100 pounds of methamphetamine by California Highway Patrol.

IV. STATEMENT OF PROBABLE CAUSE

10. Based on my review of law enforcement reports, conversations with other law enforcement agents, and my own knowledge of the investigation, I am aware of the following:

A. J.Z. Died of Fentanyl Poisoning on August 16, 2023

11. According to reports and video footage that I reviewed, I learned the following:

12. At approximately 3:00 p.m. on August 16, 2023, CPD dispatch received a call for a disoriented subject in the area of the 14700 block of Willamette Avenue in Chino, in the County of San Bernardino. Officers arrived on scene and located the reporting party, S.D., performing CPR to save J.Z.'s life. S.D. and J.Z. are both United States Postal Service ("USPS") employees who were delivering mail and packages on their respective routes.

13. During the investigation, it was discovered that J.Z. called S.D. a short time earlier and told S.D. that he did not feel well. S.D. drove to J.Z.'s location to give him water and arrived about ten minutes later. When she arrived, she found him unresponsive in the seat of his USPS vehicle (a white and red Ryder van) and was given CPR instructions by the Fire Department. When CPD officers arrived on scene, S.D. was still performing CPR. Medical personnel later pronounced J.Z. deceased at approximately 3:51 p.m.

14. During a search of J.Z.'s Ryder van, a white powder residue was found on a metal shelf in the rear portion of the van, next to the USPS fuel card. Later testing by the USPIS lab on the residue revealed that the substance contained fentanyl and cocaine.

15. When the Coroner Investigator searched J.Z. and his clothing, he located a rolled up \$100 bill with a white powder substance.

16. On October 4, 2023, I received the autopsy report from the San Bernardino County Coroner's Office, which stated that J.Z.'s cause of death was fentanyl toxicity.

B. Text Messages and Other Evidence Show that MEZA Distributed the Drugs that Killed J.Z.

17. Based on my review of reports and speaking with law enforcement personnel, I know that San Bernardino County Sheriff's Deputy Coroner and CPD detectives responded to the scene to continue the investigation. When the Coroner's Investigator was on scene, he opened J.Z.'s unlocked cell phone and located text messages to the number ending in 4552, the user of which was later identified as MEZA¹. Based on my training and experience, these messages appeared to be setting up a meeting for J.Z. to purchase narcotics from MEZA. The messages were:

- a. J.Z.: Can you drop off (11:58 AM)
- b. MEZA: Way (11:58 AM) **Where you at**
- c. J.Z.: Chino lol (12:00 PM)
- d. MEZA: Oh dang (12:01 PM)
- e. J.Z.: 80 if you want lol (12:02 PM)
- f. MEZA: Where tho (12:09 PM)

¹ As further described below, according to phone data I reviewed pursuant to a search warrant for the 4552 number, individuals referred to MEZA as "Reyes Meza" and "Reyes" in text message conversations.

g. J.Z.: 6989 Schaefer Ave, Chino, CA 91710 (12:12 PM)

h. MEZA: Omw

i. MEZA: 20 min away

j. MEZA About (all at 12:14 PM)

k. J.Z.: Ok take your time lol (12:19 PM)

l. MEZA: Here (12:36 PM)

m. MEZA: By the Pollo loco (12:37 PM)

n. J.Z.: Ok

o. J.Z.: On my way (both at 12:42 PM)

p. MEZA: Bout how long pa (12:44 PM)

q. J.Z.: 5 minutes (12:44 PM)

r. J.Z.: You got change for 100? (12:45 PM)

s. MEZA: Yeah (12:45 PM)

18. On August 17, 2023, I went to the El Pollo Loco located at 6981 Schaefer Avenue to review video surveillance of the drug deal between MEZA and J.Z. that had been arranged in J.Z.'s messages approximately three hours prior to J.Z.'s pronounced time of death. The video timestamp on the footage was about three minutes behind the actual time. The following is a summary of what I saw on the surveillance footage:

a) 12:33 PM - a red 4-door sedan, later identified as a Mercedes Benz,² arrived and parked in the north row of parking stalls, backed in.

² License plate reader hits corresponding to locations consistent with prior drug deals between MEZA and J.Z. returned a red Mercedes Benz sedan with license plate CA 8VJF230, which DMV records show MEZA as the registered owner.

- b) 12:49 PM - J.Z.'s Ryder van arrived and backed in on the driver's side of the red Mercedes, later determined to be the SUBJECT VEHICLE.
- c) 12:50 PM - J.Z. exited the Ryder van and walked up to the driver's window of the SUBJECT VEHICLE. J.Z. reached into the vehicle and then opened the sliding rood on the van. This interaction took about 15-20 seconds.
- d) 12:50 PM - The SUBJECT VEHICLE pulled out of the parking stall, exiting the complex and turning east onto Schaefer Avenue. The sedan left less than 30 seconds after J.Z. exited his Ryder van.
- e) 12:50 PM - J.Z. walked from the Ryder van and into El Pollo Loco. He went into the restroom.
- f) 12:53 PM - J.Z. left the El Pollo Loco and entered his van through the rear sliding door.
- g) 12:55 PM - the Ryder van left the parking lot.

19. The Honorable Judge Harold Wilson subsequently authored state search warrants for subscriber information and phone data related to the 4552 number (i.e., MEZA's phone) from Verizon, and a warrant to search J.Z.'s phone.

20. Based on my review of phone data obtained from Verizon for the 4552 number, I saw the message sent to J.Z. stating that MEZA had arrived at the El Pollo Loco was sent at 12:36 PM. This was the same time that the SUBJECT VEHICLE was seen arriving on the video footage that I collected from El Pollo Loco.

21. On August 24, 2023, I received information back from Verizon from the search warrant I wrote for the account

belonging to the 4552 number. There was not a name associated with the account and it appeared to be a pre-paid phone. Based on my training and experience, I know it is common for drug dealers to use pre-paid phones to limit the `paper trail` that connects them to the phone. Pre-paid phones are often used as `burner phones` which are used for a period of time until the number is discovered by law enforcement, and then often disconnected. As described below, however, text messages related to the 4552 number show that MEZA is the likely user of the phone.

22. Specifically, through my review of the Verizon information received pursuant to the search warrant, I learned the following:

a. Significant evidence showing MEZA is the user of the 4552 phone, including:

i. Incoming messages from multiple users referring to the user of the 4552 phone as "Reyes." For example, on July 24, 2023, the user with phone number ending in 4559 sends the message: "Hey Reyes this is [Individual 1]." MEZA replies with "Wzp bro". (Wzp is an abbreviation for `what's up bro`) Individual 1 proceeds to ask MEZA where he can find "a 1lb of crys," which based on my training and experience I recognize to be a pound of methamphetamine. In addition, on August 1, 2023, the user with phone number ending in 7680 asks MEZA, "what's the name for the zelle"³ and follows up with "Reyes Meza?" MEZA replies, "Yeah".

³ Zelle is an internet-based money transfer application.

ii. MEZA also mentions his home address as 12701 Lateen Drive in Moreno Valley, California,⁴ numerous times in text messages. For example, on July 29, 2023, the user with number ending in 1797 sent the message, "What's the address again" to MEZA. MEZA replied by sending "12701 lateen Dr Moreno Valley".

iii. In text messages, MEZA also mentioned he was driving his red Mercedes Benz.

iv. One of the multimedia messages from the phone appeared to be a screenshot of a payment from the CashApp payment application. The screenshot has the name "Reyes Leon Meza" at the top, with the handle of "\$reyesmz05" just underneath. The payment is for \$97.00 and lists it was "For Drew's."

b. Text messages stored by Verizon revealed a significant quantity of conversations involving the selling of drugs. MEZA coordinated multiple sales of "blues," "percs," and "30s," which I know to be counterfeit Oxycodone "m30" pills which are most commonly pressed with fentanyl. In recent years, these counterfeit pills have caused many overdoses and killed many people. I have personally investigated numerous overdose deaths that have involved blue m30 pills.

⁴ I know this is MEZA's home address because numerous police databases have MEZA's address listed as 12701 Lateen Drive, and his California driver's license lists 12701 Lateen Drive as a recent address. Moreover, during surveillance I conducted at the address on October 24, 2023, I saw him enter and exit the residence numerous times.

c. Photographs depicting suspected narcotics, including pictures of a white solidified, powder-like substance, one in rock form, and another inside a small bag on a digital scale. The scale read "0.95" which I believe is in grams. Based on my training and experience, I believe both white substances are cocaine.

C. Investigation of the SUBJECT PREMISES and the SUBJECT VEHICLE

23. I also reviewed text messages between J.Z. and MEZA from August 1, 2023 and August 16, 2023 (the date of J.Z.'s death). During my review of the messages, I noticed MEZA told J.Z. his location numerous times to arrange drug deals. Based on knowing these locations, the color, and make of MEZA's vehicle, I cross referenced these dates and times with License Plate Reading Camera systems (LPR). I noticed that the same license plate hit numerous times at these different locations, close to the listed times. The license plate was CA 8VJF230.

24. For example, on August 14, 2023, J.Z. requested that MEZA meet him at 14509 Purdue in Chino, California. MEZA told J.Z. he was about 40 minutes away at 12:58 PM. That same day, at 12:47 PM I saw an LPR hit for the red Mercedes Benz with California license plate 8VJF230 in Colton, California at N. Pepper Ave. and W. Valley Blvd. This location is about 22 miles from the meeting location of 14509 Purdue in Chino, according to Google Maps.

25. I also found an LPR hit on August 16, 2023 in Colton, California at E. Valley Blvd. and Wildrose Avenue at 13:19 PM.

This location is about 21 miles from J.Z. and MEZA's meeting location of 6989 Schaefer Avenue in Chino, California. This LPR hit was about 20 minutes prior to when the SUBJECT VEHICLE was seen pulling into the parking lot where MEZA and J.Z. met.

26. I conducted a records check of the vehicle and found it was registered to Reyes Leon MEZA at 856 S Loretta St in Rialto, California 92376. I conducted a records check of this subject and found his CA driver's license (B8838054) which had a recent address of 12701 Lateen Drive in Moreno Valley, CA 92553 ("the SUBJECT PREMISES"). I found recent LPR hits of the SUBJECT VEHICLE in the driveway and in front of 12701 Lateen Drive in Moreno Valley. Numerous police databases have MEZA's address listed as 12701 Lateen Drive.

27. On October 24, 2023, USPIS TFOs conducted surveillance at the SUBJECT PREMISES. During the surveillance, a female subject was seen entering a Dodge Charger sedan parked in the garage. She left the location and the garage door remained open. A male subject was seen walking in the garage and later closed the roll up door. A few minutes later, the same male subject, positively identified as MEZA, exited the residence through the front door, and opened a Honda Accord, bearing California license plate 7ZYY321. MEZA walked in and out of the front door of the residence about three times while placing items inside the Honda. A few minutes later, he left the residence. The Honda is registered to Daniels Used Auto in Hacienda Heights as of October 9, 2023.

28. Utilizing police databases, I discovered that MEZA was stopped by the California Highway Patrol on July 15, 2019, in the city of Beaumont. MEZA was arrested for possession/transportation of drugs for sales. I obtained a copy of the arrest report and found out that MEZA was found to be in possession of about 100 pounds of methamphetamine.

V. TRAINING AND EXPERIENCE ON DRUG OFFENSES

29. Based on my training and experience and familiarity with investigations into drug trafficking conducted by other law enforcement agents, I know the following:

a. Drug trafficking is a business that involves numerous co-conspirators, from lower-level dealers to higher-level suppliers, as well as associates to process, package, and deliver the drugs and launder the drug proceeds. Drug traffickers often travel by car, bus, train, or airplane, both domestically and to foreign countries, in connection with their illegal activities in order to meet with co-conspirators, conduct drug transactions, and transport drugs or drug proceeds.

b. Drug traffickers often maintain books, receipts, notes, ledgers, bank records, and other records relating to the manufacture, transportation, ordering, sale and distribution of illegal drugs. The aforementioned records are often maintained where drug traffickers have ready access to them, such as on their cell phones and other digital devices, and in their residences.

c. Communications between people buying and selling drugs take place by telephone calls and messages, such as e-

mail, text messages, and social media messaging applications, sent to and from cell phones and other digital devices. This includes sending photos or videos of the drugs between the seller and the buyer, the negotiation of price, and discussion of whether or not participants will bring weapons to a deal. In addition, it is common for people engaged in drug trafficking to have photos and videos on their cell phones of drugs they or others working with them possess, as they frequently send these photos to each other and others to boast about the drugs or facilitate drug sales.

d. Drug traffickers often keep the names, addresses, and telephone numbers of their drug trafficking associates on their digital devices and in their residence. Drug traffickers often keep records of meetings with associates, customers, and suppliers on their digital devices and in their residence, including in the form of calendar entries and location data.

e. Drug traffickers often use vehicles to transport their narcotics and may keep stashes of narcotics in their vehicles in the event of an unexpected opportunity to sell narcotics arises.

f. Drug traffickers often maintain on hand large amounts of United States currency in order to maintain and finance their ongoing drug trafficking businesses, which operate on a cash basis. Such currency is often stored in their residences and vehicles.

g. Drug traffickers often keep drugs in places where they have ready access and control, such as at their residence

or in safes. They also often keep other items related to their drug trafficking activities at their residence, such as digital scales, packaging materials, and proceeds of drug trafficking. These items are often small enough to be easily hidden and thus may be kept at a drug trafficker's residence even if the drug trafficker lives with others who may be unaware of his criminal activity.

h. It is common for drug traffickers to own multiple phones of varying sophistication and cost as a method to diversify communications between various customers and suppliers. These phones range from sophisticated smart phones using digital communications applications such as Blackberry Messenger, WhatsApp, and the like, to cheap, simple, and often prepaid flip phones, known colloquially as "drop phones," for actual voice communications.

VI. TRAINING AND EXPERIENCE ON DIGITAL DEVICES⁵

30. Based on my training, experience, and information from those involved in the forensic examination of digital devices, I know that the following electronic evidence, *inter alia*, is often retrievable from digital devices:

⁵ As used herein, the term "digital device" includes any electronic system or device capable of storing or processing data in digital form, including central processing units; desktop, laptop, notebook, and tablet computers; personal digital assistants; wireless communication devices, such as paging devices, mobile telephones, and smart phones; digital cameras; gaming consoles; peripheral input/output devices, such as keyboards, printers, scanners, monitors, and drives; related communications devices, such as modems, routers, cables, and connections; storage media; and security devices.

a. Forensic methods may uncover electronic files or remnants of such files months or even years after the files have been downloaded, deleted, or viewed via the Internet. Normally, when a person deletes a file on a computer, the data contained in the file does not disappear; rather, the data remain on the hard drive until overwritten by new data, which may only occur after a long period of time. Similarly, files viewed on the Internet are often automatically downloaded into a temporary directory or cache that are only overwritten as they are replaced with more recently downloaded or viewed content and may also be recoverable months or years later.

b. Digital devices often contain electronic evidence related to a crime, the device's user, or the existence of evidence in other locations, such as, how the device has been used, what it has been used for, who has used it, and who has been responsible for creating or maintaining records, documents, programs, applications, and materials on the device. That evidence is often stored in logs and other artifacts that are not kept in places where the user stores files, and in places where the user may be unaware of them. For example, recoverable data can include evidence of deleted or edited files; recently used tasks and processes; online nicknames and passwords in the form of configuration data stored by browser, e-mail, and chat programs; attachment of other devices; times the device was in use; and file creation dates and sequence.

c. The absence of data on a digital device may be evidence of how the device was used, what it was used for, and

who used it. For example, showing the absence of certain software on a device may be necessary to rebut a claim that the device was being controlled remotely by such software.

d. Digital device users can also attempt to conceal data by using encryption, steganography, or by using misleading filenames and extensions. Digital devices may also contain "booby traps" that destroy or alter data if certain procedures are not scrupulously followed. Law enforcement continuously develops and acquires new methods of decryption, even for devices or data that cannot currently be decrypted.

31. Based on my training, experience, and information from those involved in the forensic examination of digital devices, I know that it is not always possible to search devices for data during a search of the premises for a number of reasons, including the following:

a. Digital data are particularly vulnerable to inadvertent or intentional modification or destruction. Thus, often a controlled environment with specially trained personnel may be necessary to maintain the integrity of and to conduct a complete and accurate analysis of data on digital devices, which may take substantial time, particularly as to the categories of electronic evidence referenced above. Also, there are now so many types of digital devices and programs that it is difficult to bring to a search site all of the specialized manuals, equipment, and personnel that may be required.

b. Digital devices capable of storing multiple gigabytes are now commonplace. As an example of the amount of

data this equates to, one gigabyte can store close to 19,000 average file size (300kb) Word documents, or 614 photos with an average size of 1.5MB.

32. BIOMETRIC UNLOCK. The search warrant requests authorization to use the biometric unlock features of a device, based on the following, which I know from my training, experience, and review of publicly available materials:

a. Users may enable a biometric unlock function on some digital devices. To use this function, a user generally displays a physical feature, such as a fingerprint, face, or eye, and the device will automatically unlock if that physical feature matches one the user has stored on the device. To unlock a device enabled with a fingerprint unlock function, a user places one or more of the user's fingers on a device's fingerprint scanner for approximately one second. To unlock a device enabled with a facial, retina, or iris recognition function, the user holds the device in front of the user's face with the user's eyes open for approximately one second.

b. In some circumstances, a biometric unlock function will not unlock a device even if enabled, such as when a device has been restarted or inactive, has not been unlocked for a certain period of time (often 48 hours or less), or after a certain number of unsuccessful unlock attempts. Thus, the opportunity to use a biometric unlock function even on an enabled device may exist for only a short time. I do not know the passcodes of the devices likely to be found in the search.

c. Thus, the warrant I am applying for would permit law enforcement personnel to, with respect to any device that appears to have a biometric sensor and falls within the scope of the warrant: (1) depress MEZA's thumb and/or fingers on the device(s); and (2) hold the device(s) in front of MEZA's face with his or her eyes open to activate the facial-, iris-, and/or retina-recognition feature.

2. Other than what has been described herein, to my knowledge, the United States has not attempted to obtain this data by other means.

VII. CONCLUSION

33. For all of the reasons described above, there is probable cause to believe that MEZA has committed a violation of 21 U.S.C. § 841(a)(1), (b)(1)(C): Distribution of Fentanyl Resulting in Death. There is also probable cause that the items to be seized described in Attachment B will be found in a search of the SUBJECT PREMISES, SUBJECT VEHICLES, and the person described in Attachments A-1, A-2, and A-3.

Attested to by the applicant in accordance with the requirements of Fed. R. Crim. P. 4.1 by telephone on this 3rd day of November, 2023.



THE HONORABLE SHERI PYM
UNITED STATES MAGISTRATE JUDGE